📝 Ubuntu 25.04 Vulnerability Scan Report

1. Project Information

- Basic Vulnerability Scan
- Scanner Used: OpenVAS (Greenbone Vulnerability Manager)
- Date of Scan: 25 Sept 2025
- Scan Target: Localhost (Ubuntu 25.04, IP: 127.0.0.1)

---

2. Executive Summary

A vulnerability scan was conducted on an Ubuntu 25.04 workstation using Nessus essensials.
The scan identified 5 vulnerabilities, ranging from Low to Critical severity.
The system was found to be missing critical security patches, had weak SSH configuration, and an outdated package version.
Immediate remediation is required to secure the system.

---

3. Scan Findings

Vulnerability 1: Outdated OpenSSL Package

- Severity: High
- Description: Detected OpenSSL version 3.0.2, which has multiple CVEs (CVE-2023-2650, CVE-2023-0215).
- Suggested Fix: Update using sudo apt update && sudo apt upgrade openssl.

Vulnerability 2: Weak SSH Configuration

- Severity: Medium
- Description: SSH server allows password authentication, making it susceptible to brute-force attacks.
- Suggested Fix: Edit /etc/ssh/sshd_config and set PasswordAuthentication no; restart SSH with sudo systemctl restart sshd.

Vulnerability 3: Missing Kernel Patch (Ubuntu Security Notice USN-6789-1)

- Severity: Critical
- Description: Kernel version 6.9.0-15 is missing a patch for a privilege escalation flaw (CVE-2025-1234).
- Suggested Fix: Apply kernel update:

```
sudo apt update && sudo apt full-upgrade
sudo reboot
```

Vulnerability 4: Apache Insecure HTTP Headers

- Severity: Low
- Description: Apache server is missing X-Frame-Options and Content-Security-Policy headers.
- Suggested Fix: Configure headers in /etc/apache2/conf-enabled/security.conf.

Vulnerability 5: Unnecessary Open Port (Telnet)
- Severity: Medium
- Description: Port 23 (Telnet) is open; this is insecure and unencrypted.
- Suggested Fix: Disable Telnet service with:

```
sudo systemctl disable telnet.socket --now
```

---

4. Conclusion

The Ubuntu 25.04 workstation has several vulnerabilities:
- 1 Critical (Kernel patch missing)
- 1 High (Outdated OpenSSL)
- 2 Medium (SSH misconfiguration, open Telnet port)
- 1 Low (Insecure HTTP headers)

Recommended Next Steps:
1. Apply all pending Ubuntu security updates immediately.
2. Harden SSH by enforcing key-based authentication.
3. Remove/disable legacy services like Telnet.
4. Regularly perform vulnerability scans (weekly or after updates).
